Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Rules and Regulations Implementing the Truth in Caller ID Act of 2009	)	WC Docket No. 11-39
	)	

COMMENTS OF TELTECH SYSTEMS, INC.

Summary

TelTech Systems, Inc. ("TelTech") offers these comments on certain issues raised by the Commission's notice of proposed rulemaking ("NPRM") to implement the Truth in Caller ID Act of 2009 (the "Truth in Caller ID Act" or the "Act").1

If the Commission decides to adopt rules imposing record keeping or reporting obligations on providers of caller ID spoofing services, those rules may not be limited to third party providers of caller ID spoofing services to businesses and individuals. Rather, such obligations must be imposed across the board, on all entities engaging in or providing caller ID spoofing capability to third parties, whether those third parties are paying customers, employees or others. The NPRM identifies three types of obligations that could potentially be imposed on caller ID spoofing service providers: (1) record keeping requirements, (2) the duty to verify a user's right to spoof a particular number, and (3) reporting requirements. TelTech would have no objection if the Commission chose to adopt reasonable record keeping obligations, so long as they were limited in scope and focused on data concerning the calls placed by users. However, any rule imposing verification or reporting obligations would not be legally justified, effective or designed to further the purposes of the Act.

[1] Truth in Caller ID Act of 2009, Pub. L. No. 111-331, codified at 47 U.S.C. § 227(e).

The Truth in Caller ID Act does not require that a caller have the right to use the spoofed or substituted number, so the Commission has to date correctly decided not to impose a verification requirement. It should hold to that course now. Verification should not be required because it would be pointless, not to mention ineffective and expensive. Using a number that you do not have permission to spoof is not illegal under the Act. In fact, the Act's legislative history specifically recognizes that legitimate uses of spoofing may involve situations where the caller is deliberately misleading by hiding his identity, including by using a number which he or she may have no authorization to spoof.

The Commission must be very careful about imposing any reporting requirements on providers of spoofing services. In theory, reporting requirements would be a simple way to assist law enforcement. In practice, as TelTech's experience detailed below shows, identifying and reporting suspected criminal activity is a difficult and complex process fraught with legal ambiguity and risk. TelTech recognizes that the legal posture of and possible risk to a reporting entity might arguably be somewhat different if the Commission were to impose a reporting requirement. However, it urges the Commission to consider all facets of the problem and to consult closely with the FBI and the Criminal Division of DOJ before imposing any sort of reporting requirements.

The Commission's rules should create an explicit exemption from liability under the Act for providers of caller ID spoofing services. Congress did not intend to create liability for service providers – whether carriers, interconnected VOIP providers, information service providers such as TelTech, or businesses operating PBXes - that are merely transmitting information selected by a caller. Since Congress did not intend to impose service provider liability under these circumstances, the rules should be modified to clarify this exemption. Such

an explicit expression will prevent confusion and help small businesses by minimizing unnecessary litigation and expense down the road.

The NPRM also sought comment on what rules the Commission can adopt to discourage or prevent caller ID spoofing services from enabling or facilitating unlawful conduct. No such rules are necessary at this time because third party spoofing service providers are taking steps on their own to combat unlawful conduct. TelTech, for example, already works with public agencies and private entities to deter unlawful conduct by users. TelTech cooperates with law enforcement agencies in providing information about ongoing criminal activity, identifying new types of criminal activity and developing innovative anti-fraud techniques.

The NPRM also asked whether there ways that carriers and interconnected VoIP providers can prevent third parties from overriding calling parties' privacy choices. It is not clear why this question was raised in the NPRM, since the Commission has for decades allowed third parties to override parties' privacy choices in called-party-pays situations and nothing in the Truth in Caller ID Act addresses this unmasking issue or gives the Commission any new legal authority to address this practice. If the Commission believes that other provisions of the Communications Act provide it with the necessary authority to address this issue, then the proper course of action would be to publish an NPRM identifying those provisions and any proposed rules.

Finally, TelTech believes that the delivery of caller identification information to E911 public safety answering points should be considered a type of "Caller Identification Service" for purposes of the new rules. TelTech has blocked calls to 911 since 2006, and there is no reason every provider should not do so.

Table of Contents

Introduction

TelTech owns and operates SpoofCard.com, an information service that provides, among other capability, the ability to replace or "spoof" the caller ID on a telephone call. To place a call using the SpoofCard service, a customer must call one of TelTech's toll free numbers (also known as an 800 or Direct Inward Dialing ("DID") number). The customer normally initiates a call on the public switched telephone network ("PSTN") using TDM protocol (i.e., a "regular phone call"), although some customers may initiate a call from a computer or other device using IP technology. On a regular phone call, the caller ID is transmitted as one of the fields in the Signaling System 7 ("SS7") out-of-band signaling scheme. If the call is initiated in IP format, it is converted at some point to TDM protocol before reaching TelTech's DID provider. On an IP call, the computer or other device ordinarily transmits a set of numbers in session initiation protocol ("SIP") that can be converted into a caller ID data field in SS7.

The call is directed by the originating local exchange carrier ("LEC") (or the broadband service provider, if it is an IP call) to the network carrier that TelTech uses for its DID numbers. The DID service provider converts the TDM call to IP format and delivers the call to SpoofCard's virtual servers operated on a third party's cloud services platform. TelTech runs the service on the cloud servers using the free Asterisk open source software, along with some modified open source calling card scripts that TelTech programmers wrote. TelTech stores its call and sales data in MySQL databases on the cloud servers.

When the customer's call reaches the server, the program prompts the customer to enter her personal identification number ("PIN") in order to begin the call process. The customer then also enters her desired caller ID (the "spoofed" caller ID) and the number she wishes to call, and chooses whether she wishes to record the call or to use other features of Asterisk. The Asterisk

software has the functionality to change the "Calling Party Number" or CPN field on outbound IP calls, with SIP as the signaling protocol.

After the customer has made her choices, the Asterisk program re-directs the call back to TelTech's wholesale VOIP termination provider. When the IP call is converted back to TDM for termination, the SS7 Caller ID field is derived from the SIP CPN field. TelTech's wholesale carrier delivers the call (directly or through another carrier) to the terminating LEC serving the called party. The IP signal is converted to TDM by either the wholesale VOIP provider or the terminating PSTN carrier, and the call is completed to the called party.

Issues Raised in the NPRM

A. If Any Obligations Are Imposed, They Must Apply to All Providers of Caller ID Spoofing Capability

Paragraph 21 of the NPRM invites comments "on whether [the Commission] can and should adopt rules imposing obligations, including record keeping and reporting obligations, on providers of caller ID spoofing services when they are not themselves acting with intent to defraud, cause harm, or wrongfully obtain anything of value." If the Commission does impose any such obligations, they may not be limited to third party providers of caller ID spoofing services to businesses and individuals. Rather, such obligations must be imposed across the board, on all entities engaging in or providing caller ID spoofing capability to third parties, whether those third parties are paying customers, employees or others.

There is no basis in the Act for distinguishing between spoofing enabled by what the NPRM refers to as "third party spoofing services providers" and spoofing enabled or carried out by any other enterprise, carrier or individual that operates hardware or software that is capable of spoofing. As the NPRM notes,

> The proposed rules prohibit any person or entity acting with the intent to defraud, cause harm, or wrongfully obtain anything of value from knowingly causing a caller ID service to alter or manipulate caller ID information. That prohibition does not distinguish between large businesses and entities, small businesses and entities, or individuals.
>
> NPRM, para. 12.

As the NPRM recognized, there are now numerous third party providers of caller ID spoofing services, which makes it easy for callers to engage in caller ID spoofing. For example, more than 5 million businesses and individuals have downloaded and are presumably using the open source Asterisk software that TelTech uses.[2] In addition to these users, many other types of entities provide caller ID spoofing services using a variety of other hardware and software.[3] The fact is that today neither service providers nor called parties can determine whether the caller ID information they receive is accurate. More importantly, there is no easy fix to change that situation. Singling out one small subset of the myriad of entities that provide spoofing capability is both discriminatory and guaranteed to be ineffective.

B. No Duties Other Than Record Keeping Obligations Can or Should Be Imposed

The NPRM identifies at three types of obligations that could potentially be imposed on service providers: (1) record keeping requirements, (2) the duty to verify a user's right to spoof a particular number, and (3) reporting requirements.

Narrowly drawn record keeping requirements might be acceptable. However, any rule imposing verification or reporting obligations would not be legally justified, effective in practice or designed to further the purposes of the Act.

---

[2] See www.asterisk.org.

[3] For example, some companies offer "caller identification management services" to business clients and make it possible for those customers to transmit different, locally-based CPNs to different geographic areas.

1. The Commission Could Impose Reasonable Record Keeping Requirements

TelTech would have no objection if the Commission chose to adopt reasonable record keeping obligations for providers of caller ID spoofing capability, so long as they were limited in scope and focused on data concerning the calls placed by users. Any such record keeping requirements should not be unduly burdensome for TelTech or most other third party spoofing service providers, regardless of the provider's size. As discussed in the preceding section, however, any record keeping requirement that the Commission might impose should be applied not just to third party service providers, but across the board to all providers of spoofing services, including entities such as interconnected VOIP providers and businesses running their own PBXes.

TelTech already maintains detailed records of all calls placed through its system. The Asterisk program used by TelTech creates a call detail record ("CDR") similar to, but more detailed than, the CDR created by a Class 5 switch using the Signaling System 7 ("SS7") protocol on the PSTN. An Asterisk CDR contains not only the usual PSTN CDR fields - calling number, ANI, called number, time of call initiation, etc. – but also fields for data such as (i) the spoofed number, (ii) whether the caller changed his or her voice using the voice change function, (iii) whether the caller recorded the conversation, and several other data points. If the caller did record the conversation, the Asterisk CDR will also contain a field linking to the recording.

TelTech presently maintains these CDRs (and the associated call recordings created by the customer) indefinitely.[4] Given the level of detail in the CDRs and the length of time that TelTech retains them, TelTech's call database is a valuable tool for law enforcement agencies, as discussed in Section B(3) below.

[4] Recordings are stored on the servers running the Asterisk program until they are deleted by the customer.

It is important to distinguish between record keeping related to calls placed through the service and record keeping related to users of the service. The great majority of TelTech's customers sign up for the service online through the website, and they use credit cards to pre-pay for the service. As to these customers, TelTech has relatively complete information, usually including, among other data, the name, billing address and credit card number and the IP address of the computer from which the purchase was made. However, TelTech also sells pre-paid cards for the SpoofCard and other services. These cards are sold to wholesalers, who then resell them to retailers for sale in kiosks, grocery stores and other retail outlets. Like cards offered by sellers of long distance ("LD") and SIM cards used in pre-paid phone services, the TelTech cards provide purchasers with a password or personal identification number ("PIN") that is used to access the SpoofCard system. However, also like sellers of pre-paid LD and SIM cards, TelTech has no further information about the purchaser of the card. More importantly, it has no way of obtaining accurate information about that hard card purchaser during the use of the SpoofCard service.

The Commission should not (and probably lacks jurisdiction to) impose obligations related to collection of user data. Thus, the Commission should not impose on third party service providers any requirement that they collect specific identification information from all of their customers. If the Commission were to implement regulations requiring such detailed record keeping about all customers, TelTech and many other providers of services with spoofing capabilities would be forced to change their business model and probably to abandon retail sales of hard cards. The impact on small businesses such as TelTech would be devastating.

2. There is No Justification for Nor Any Legal Basis to Impose a Verification Requirement

The Department of Justice ("DOJ") has urged the Commission to consider adopting rules requiring "public providers of caller ID spoofing services to make a good-faith effort to verify that a user has the authority to use the substituted number, such as by placing a one-time verification call to that number."[5] Some members of the House of Representatives urged the Commission to consider adopting a similar verification requirement during the debate over the Truth in Caller ID Act on the House floor.

The Commission has to date correctly decided not to impose a verification requirement. It should hold to that course now. Verification should not be required because it would be pointless, not to mention ineffective and expensive.

Verification (particularly a single initial verification of the sort suggested by the DOJ) cannot establish the caller's intent on a specific call, and has no relationship to detecting violations of the Act. Any regulation that required verification would be neither required by nor consistent with the language of the Act. It also would not be designed to achieve any goal of the Act. The Act does not require that a caller have the right to use the spoofed or substituted number. To put it another way, using a number that you do not have permission to spoof is not illegal under the Act. In fact, the Act's legislative history specifically recognizes that legitimate uses of spoofing may involve situations where the caller is deliberately misleading by hiding his identity, including by using a number which he or she may have no authorization to spoof.[6] Neither the FCC nor the service provider will know whether a caller has the necessary criminal intent merely from a verification of his or her right to use a particular number, whether the

[5] Letter from Lanny A. Breuer on behalf of the Department of Justice to Marlene Dortch, Jan. 26, 2011 at 4.

[6] See, e.g., statements of Reps. Stearns, Engel and Boucher, Cong. Record H8378-8380 (Dec. 15, 2010).

verification occurs once at the time of customer sign-up or is repeated prior to each call placed by a customer.

Moreover, none of the proponents of verification has identified what, if anything, could or should be done if a caller failed verification. Verifying whether a user has the authority to use the spoofed number would in fact be a pointless exercise. If the caller failed verification, the service provider would have no duty to prevent the call from going through to the called party.[7] In fact, if the service provider were a licensed provider of telecommunications services (i.e., a common carrier), it would probably violate the Communications Act if it blocked or failed to complete the call.

Verification proposals are simply not well thought through. A verification requirement would be nothing more than a thinly disguised attempt to force service providers to do indirectly what neither Congress nor the Commission can do directly – limit the speech of callers by preventing them from spoofing when they have no specific criminal intent.

3. Reporting Requirements Must be Considered Carefully, as They Could Expose Service Providers to Potential Liability and Raise Insoluble Problems

The Commission must be very careful about imposing any reporting requirements on providers of spoofing services, particularly since the requirements would have to be imposed on all providers (see Section A above). In theory, reporting requirements would be a simple way to assist law enforcement. In practice, as TelTech can attest, identifying and reporting suspected criminal activity is a difficult and complex process fraught with ambiguity. Even where a

[7] The one exception might be where the service provider knew the call was illegal – i.e., where it also knew that the caller had the intent to defraud or cause harm. However, it is unclear how a service provider would have this knowledge unless it were actually monitoring the content of its customers' calls in real time.

service provider knows or has reason to know of possible illegal conduct by a customer, there are legal issues related to reporting that are likely beyond the power of the Commission to address.

TelTech has a high degree of familiarity with the issue of reporting customers' criminal activity that is directed at it or at third parties. TelTech has since early in SpoofCard's operation conducted an evolving and multifaceted fraud detection system to protect itself. As a result, TelTech frequently also becomes aware of fraudulent or other criminal activity that is targeted at third parties. For example, criminals who use a stolen credit card to purchase SpoofCard minutes will also often use the service to try to commit identity theft or financial fraud (such as facilitating fraudulent Western Union money transfer transactions).

This fraud detection system was instituted because TelTech found that many SpoofCard accounts were being opened online with fraudulent credit cards. Such fraudulent transactions caused TelTech financial harm in two ways. First, TelTech had to pay its suppliers for the minutes used by the perpetrators, and it never received payment because the banks rejected TelTech's initial charges on the fraudulent cards. Second, at the time that banks reject a fraudulent credit card charge, they also impose a "chargeback," which is similar to a bounced check charge and can be as much as $35 per transaction. In 2006, TelTech incurred tens of thousands of dollars in telecommunications costs and chargebacks related to fraudulent accounts, and its rate of chargebacks was so high that its credit card company cancelled its merchant account and TelTech had to find a new credit card company.

As its losses mounted in 2006, TelTech developed an internal system to identify suspected fraudulent accounts. Initially, when an account was determined to be fraudulent, it was terminated. However, TelTech found that this action only exacerbated its losses, because many perpetrators simply opened another account using a different fraudulent credit card, and

the cycle repeated itself. TelTech still paid for the minutes the perpetrators used, plus it had even more losses because of the increased number of chargebacks. It therefore modified the fraud detection and prevention system and began looking at other factors, including the account call pattern.

In the course of implementing this internal fraud prevention program, TelTech discovered that several dozen customers were making calls where the called number and the spoofed caller ID were identical. TelTech realized that they were calling numbers that belonged to others and accessing these third parties' voicemails without permission. As far as TelTech could determine, the called numbers were on the T-Mobile network. That network, like other mobile networks, reads the caller ID string and - if it is the same as the called number - forwards the call directly into the voicemail system. Unlike other mobile networks, T-Mobile's default mode did not require a password on a voicemail account, so a caller did not need to put in a password to listen to voicemails once the network forwarded his call to voicemail. In hopes of stopping the spoofing callers' behavior, which appeared to violate federal law, TelTech terminated the customers' accounts, sent them an email explaining the reason, and issued a press release announcing the action.[8] TelTech also contacted counsel for T-Mobile to inform them of the vulnerability of the T-Mobile system; it is unclear whether T-Mobile changed its password policy.

Through its internal fraud identification program, TelTech has also identified other accounts that are apparently being used to commit crimes, primarily financial crimes (money transfer fraud or activation of stolen credit cards) or identity theft. Since such activity was and is in violation of the terms of use to which all customers agree, TelTech considered whether to

[8] See http://www.teltechcorp.com/news/.

make voluntary disclosure of its customers' conduct to law enforcement. Before doing so, it consulted with outside counsel that specialized in electronic disclosure, privacy and criminal issues. TelTech became aware that there was substantial legal risk to it if it chose voluntarily to report such activity by its customers to law enforcement. TelTech also discussed the issue with representatives of the FBI and other federal law enforcement agencies. They informed TelTech that they were not aware of any federal statute or regulation that permits TelTech to make such voluntary disclosures without creating risk (both legal and financial (i.e., possible litigation costs)) for TelTech. In addition, they expressed concerns that an ongoing program of disclosure without a search warrant or subpoena could raise search and seizure issues under the Sixth Amendment to the U.S. Constitution. As a result, TelTech made the business decision not to risk making such voluntary disclosures.

TelTech recognizes that the legal posture might arguably be somewhat different if the Commission were to impose a reporting requirement. However, it urges the Commission to consider all facets of the problem and to consult closely with the FBI and the Criminal Division of DOJ before imposing any sort of reporting requirements.

Even if the Commission could ensure that service providers reporting their customers' suspected criminal activity would have neither potential liability nor additional costs from defending customer lawsuits, there are also enormous practicable hurdles to consider. A reporting requirement would be impossibly complex to administer. First, what level of suspicion would justify or compel reporting by a service provider? Would all types of suspected crimes be reportable, or would providers only have to report serious criminal activity such as fraud? To whom would service providers have to report the activity? Few, if any, crimes would fall under the Commission's jurisdiction, so reporting customers' criminal activity to the Commission

would not make sense. If not to the Commission, to whom would suspected criminal activity be reported? Service providers lack the expertise and resources to determine whether most suspected criminal activity is potentially a state or federal offense. Even if a service provider were able to correctly conclude that criminal activity was potentially a federal offense, how would it determine to which agency or DOJ office the activity should be reported? If the activity were potentially a state offense, how would a provider determine which state or states (and which agency within a state) might potentially have jurisdiction?

C. Service Providers Should Be Exempt From Liability For Their Users' Spoofing

The Commission seeks comment on how to interpret the statutory language prohibiting any person from "*causing any caller identification service to knowingly transmit* misleading or inaccurate caller identification information with the intent to defraud, cause harm or wrongfully obtain anything of value." NPRM para. 13 (emphasis added). It also seeks comment on whether it should "more generally exempt conduct by carriers or interconnected VoIP providers that is necessary to provide services to their customers." *Id.*, para. 23.

It is clear that Congress did not intend to create liability for service providers – whether carriers, interconnected VOIP providers, information service providers such as TelTech, or businesses operating PBXes - that are merely transmitting information selected by a caller. To that end, the quoted language from Section 227(e) refers only to the knowledge of the actor causing the caller identification service to transmit the inaccurate information. The proposed rules thus correctly require that the person or entity prohibited from "knowingly" causing transmission or display of inaccurate or misleading caller identification information must be the same person or entity acting with intent to defraud, cause harm, or wrongfully obtain anything of value. The operator or provider of the caller identification service ordinarily has no way of

knowing whether or not the caller has "the intent to defraud, cause harm or wrongfully obtain anything of value," so the service provider itself cannot have such intent and thus cannot be in violation of the Act.[9] Therefore, the proposed rules accurately reflect Congress' intent and should not be changed.

However, the proposed rules do not go far enough. The Act gives the Commission the authority to adopt additional exemptions to the prohibition on using caller ID spoofing if it determines them to be appropriate.[10] The Commission should exercise this authority by adopting a rule making clear that any provider of spoofing services – whether a common carrier, an interconnected VoIP provider or an information services provider such as TelTech - is exempt from liability under the Act *unless the service provider itself has the intent to defraud, cause harm or wrongfully obtain anything of value*. Absent such intent, a "carrier or provider merely transmits the caller ID information it receives from another carrier, provider, or customer" (NPRM at para.) and cannot have the requisite intent to violate the Truth in Caller ID Act. Congress clearly did not intend to impose service provider liability under these circumstances, and therefore the rules should make this clear. Such an explicit expression will prevent confusion and help small businesses by minimizing unnecessary litigation and expense down the road.

If the Commission adopts a general rule that exempts service providers from liability for transmitting false caller ID information except where they have the intent to defraud, cause harm, or wrongfully obtain anything of value, then a specific provision that exempts service providers

[9] The exception would be the narrow circumstances discussed in footnote 7 above.

[10] Section 227(e)(3)(B)(i).

for their conduct that is "authorized or required by law" should be unnecessary. *See* NPRM at para. 13 and 23.

D. Service Providers Are Already Developing Techniques to Combat Users' Unlawful Conduct, So No New Additional Rules Are Necessary

The NPRM also sought comment broadly "on what rules [the Commission] can adopt to discourage or prevent caller ID spoofing services from enabling or facilitating unlawful conduct." *Id.* at para. 21. No such rules are necessary at this time because third party spoofing service providers are taking steps on their own to combat unlawful conduct. TelTech, for example, already works with public agencies and private entities to deter unlawful conduct by users.

TelTech cooperates with law enforcement agencies in providing information about ongoing criminal activity, identifying new types of criminal activity and developing innovative anti-fraud techniques. TelTech regularly responds to search warrants, subpoenas, national security letters, and other forms of valid legal process (collectively, "Subpoenas") from state and federal law enforcement and national security agencies requesting information about the activity of particular accounts. On average, the TelTech responds to about two Subpoenas per week, and more than one hundred per year. In addition, TelTech responds to many additional informal requests from law enforcement. In many such requests, the agency initially contacts TelTech to determine if it has records showing that its system was used to call or spoof a certain number. If TelTech confirms that it has relevant data, the law enforcement agency usually serves a subpoena for the records on TelTech.

TelTech has also taken pro-active steps to discourage and halt unlawful conduct. For example, it has co-operated on an ongoing basis with the FBI and the Computer Crime and

Intellectual Property Section ("CCIPS") of the Criminal Division of the DOJ in educating federal law enforcement and intelligence personnel about the operation of the Asterisk technology, the uses that customers are making of the technology, and the types of illegal conduct (including fraud against third parties) that TelTech is seeing in its business. The first educational meeting with representatives of CCIPS and the FBI occurred in the summer of 2006, and a larger meeting with personnel from the DOJ, FBI, CIA, NSA, DEA and the Treasury Department was held in Washington, D.C. in the fall of 2006. Follow up conversations and another meeting with CCIPS and FBI personnel took place in the fall of 2007. In addition, TelTech personnel have subsequently held training sessions for prosecutors in Manhattan and for the U.S. Marshall Service, and its CEO frequently speaks at and attends the quarterly meetings of the Secret Service Electronic Crimes Task Force, which is based in the New York tri-state area and consists of federal law enforcement agencies.

TelTech also responds to numerous subpoenas from private parties that call for production of call detail records. TelTech is also working with the private sector to develop innovative anti-fraud techniques. In 2007, TelTech was approached by a large private sector trusted entity that provides identity and transaction verification services to governments, very large financial entities and other large enterprises. TelTech entered into a contract with this entity to provide it with real-time information about the spoofed and called number on calls being made using the SpoofCard service. No customer-specific data is disclosed. The trusted entity uses this data on a real-time basis to advise its clients whose numbers are being called about whether a particular caller is likely to be who he or she claims to be. The trusted entity and its clients also use this data to identify "deflected fraud" and "successful fraud (i) for post-transaction review and analysis of performance metrics and (ii) to design better systems for fraud

detection going forward. Since TelTech entered into this contract, it has noticed a significant drop in spoofed calls on its system to the toll-free numbers of certain large financial institutions.

E. The Proposed Rules Should Not Address Consumer-Focused Caller ID Unmasking Services

The NPRM noted that some entities also offer the ability to unmask a blocked number, effectively stripping out the privacy indicator chosen by the calling party. It asked whether there are ways that carriers and interconnected VoIP providers can prevent third parties from overriding calling parties' privacy choices. NPRM at para. 27.

TelTech is commenting on this issue because it also offers the innovative TrapCall service (see www.trapcall.com) , which for the first time provides individual customers the ability to unmask a blocked number on a per call basis. It is unclear why the question in para. 27 is being asked, since the Commission has for at least two decades allowed individuals and entities that purchase called-party-pays or reverse charge services (e.g., 800, 866, and 888 numbers) to override calling parties' privacy choices, identify the calling party, and use that information for caller identification, customer marketing and other purposes. As the Commission is aware, having investigated TrapCall after it was first offered in 2009, the TrapCall service simply makes available to individuals one of the benefits of a called-party-pays service that has long been available to businesses. Nothing in the Truth in Caller ID Act addresses this unmasking issue or gives the Commission any new legal authority to address this practice when it is engaged in by parties (collectively, "non-telecom providers") that are neither carriers nor interconnected VoIP providers. In any event, TelTech is not aware of any technological means by which carriers, interconnected VoIP providers or non-telecom providers can prevent some third parties from overriding calling parties' privacy choices.

If the Commission believes that other provisions of the Communications Act provide it with the necessary authority to prevent all third parties from overriding calling parties' privacy choices, then the proper course of action would be to issue an NPRM identifying those provisions and any proposed rules. TellTech has not investigated, and has no comment on, whether the Commission could propound rules to prohibit all non-telecom providers (including individuals and business using 800, 866, and 888 numbers) from overriding calling parties' privacy choices and using the unmasked data internally or distributing it for external use.

F. The Proposed Rules Should Prohibit the Transmission of A Spoofed Number to E911 PSAPs

The delivery of caller identification information to E911 public safety answering points should be considered a type of "Caller Identification Service" for purposes of the new rules. Transmitting spoofed caller identification information to emergency services providers (often referred to as "swatting") is a particularly dangerous practice, and one which Congress was particularly concerned about when adopting the Truth in Caller ID Act.

TelTech has been a leader in combating this nefarious practice. Since 2006, TelTech has blocked all spoofed calls to "911." This is a simple task, requiring just a few lines of code in the Asterisk program. Any responsible provider of third party spoofing services should have already adopted this policy. Similarly, TelTech's system will not allow any caller to use "911" as a spoofed number, because it requires a ten digit number for spoofing.

However, it would be nearly impossible as a practical matter to outlaw or prevent all spoofing on calls directed to E911 public safety answering points or to local police or fire stations. These agencies can also be reached on non-emergency numbers other than "911," and a number of callers have committed "swatting" by calling local police non-emergency numbers

(instead of 911) to report false emergencies that lead to the dispatch of SWAT teams or fire equipment to the residences of innocent third parties. The only way to limit this practice would be to compile a database of federal, state and local law enforcement and fire numbers and make it available to spoofing services providers for use on a voluntary or mandatory basis.[11] Such an undertaking would require an extraordinary public/private effort.

Conclusion

The proposed rules should be adopted (subject to being amended as suggested above) and applied to all providers of caller ID spoofing services.

Respectfully submitted,

_____/s/_____

Mark C. Del Bianco

Counsel for TelTech Systems, Inc.

Law Office of Mark C. Del Bianco
3929 Washington St.
Kensington, MD 20895
Tel: 301-933-7216
mark@markdelbianco.com

Date: April 18, 2011

[11] Such a list could be included both in a "do not spoof" blacklist and a "blocked numbers" or "do not call" blacklist. TelTech presently implements both types of lists in its system. Its "do not spoof" list, for example, contains over 4500 numbers, the majority being numbers provided by law enforcement agencies and most of the remainder coming from financial institutions.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on this 18th day of April, 2011, a true and correct copy of the foregoing Comments was served electronically on the following:

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington D.C. 20554
(**via ECFS filing**)

Best Copy and Printing, Inc.
Portals II
445 12th Street, S.W.
Room CY-B402
Washington, DC 20554
fcc@bcpiweb.com

Competition Policy Division
Wireline Competition Bureau
Federal Communications Commission
445 12th Street, S.W.
Washington D.C. 20554
cpdcopies@fcc.gov

/s/
Mark C. Del Bianco